

Ubuntu CD/DVD Encryption

By: KenTheFurry

Email: KenTheFurry@gmail.com

GPG Key: 068ACDD2

Requirements

To be able to do this tutorial you will need to make sure that you have these things...

CD/DVD burning software

A Blank CD/DVD

Cryptsetup

Access to a sudo account

And finally some time

Forward

My method is alot simpler that it looks; once you have done it a few times you will have it down and it will become very easy to do from scratch without my tutorial.

Feel free to improve on my method all you want; you should always try to push the bar and do something that has never been done before.

Why?

Why might you want to be able to make encrypted CDs you may ask.

There are many reasons someone may want to encrypt the contents of a disk...

A possible reason to make encrypted disks could be to store my downloaded Movies; the ones I like but don't want them taking up space on my Hard Drive.

Tutorial

First off we will need to create a work directory(a directory where we will be storing the files we are working with)

I would place it on your Desktop.

First Open a Terminal(Ctrl+Alt+T)

Now lets cd into our Desktop.

```
cd Desktop
```

Now we need to make our work directory...

```
mkdir tmp0
```

```
cd tmp0
```

Now we need to make a file that will be our file system...

```
dd if=/dev/zero of=CD.iso bs=1M count=700
```

Now lets break down this command...

dd is a program for copying bytes of information.

if means Input File. (our input is from the zero generating file all it returns is 00)

of means Output File.

bs means Buffer Size (1M means one MB so each time it runs it will grab 1MB of zeros)

count means the amount of times to grab bs amount of zeros. End file

size=bs*count

Ok so now if we look in our work directory we will find that we have a iso file that is 700MB in size.

Now we need to setup the file into a loop device.

But to do this we need to know the address of an empty loop device...

So we do this command...

```
sudo losetup -f
```

For me it was `/dev/loop3`, it may be different for you.

So now we need to mount that file as a loop device...

```
sudo losetup /dev/loop3 CD.iso
```

Now we can set that device up as a encrypted file system.

This is where you can choose your method of encryption I personally like

Twofish but you should do a search on what encryption methods your computer supports and pick for yourself...

What ever encryption you use make sure you add `-cbc-essiv:sha256` to the end of it... You can do a search as to why if you want; I'm not going to go into it.

Encrypt the filesystem...

```
cryptsetup -c twofish-cbc-essiv:sha256 -h whirlpool -s 256 luksFormat  
/dev/loop3
```

Here is the break down of this command lol...

Cryptsetup is a encrypted device program kinda...

-c allows you to change the default cipher

-h lets you choose the hash I use whirlpool I love it but do a search for others and find one you like.

-s allows you to change the default key size the default is only 128, 256 is more secure.

LuksFormat tells cryptsetup to pass all your vars over to the luksFormat.

Follow through with the steps for cryptsetup it will tell you what to do.

Choose a strong password. And remember to never give your password away to anyone, Never use a simple password. Look up good passwords and do not use them. The weakest part of a encrypted file system will always be the password.

Think about it...

If you were using an 40 bit key, keep in mind bits are 1s and 0s it could look like...

11111111 00000000 11111111 00000000 10101010

So because there are only 2 options for each slot for every extra bit the number of all possible keys goes up by a huge number.

The formula for that is... $2^{\text{bit size}}$, so for a 40 bit key that would be $2^{40}=1,099,511,627,776$ if you bump that up to a 128 bit key...

340,282,366,920,938,463,374,607,431,768,211,456

A 128 bit key is the default but I set it to 256... Do the math.

Ok so now you have an idea on just how secure the key is...

Now lets look at cracking your password and how a brute forcer may do it...

Lets say your password is only five characters long.

That is about the normal(I use a 60 digit pwd with nums chars upper and lower when I can) ok well think about it the normal person only uses A-Z,a-z,and/or 0-9

So that means there are $26+26+10=62$ possible characters for each slot, if the password was only one character long there would be only 62 possible characters for it... But for a five char password... $62^5 = 916,132,832$

A fairly big number right? But which would take less time 40 bit key(1,099,511,627,776) or a five digit password (916,132,832).

So I guess the point of that was choose a good password, do not choose a word or a few words joined together because there are programs that can load a dictionary and go through every word in it in different ways and if your password is a word it will be found. I would use a password that has special characters in it !@#\$%^&*()_+ -=[]{};':",. ?<>, etc and numbers and letters upper and lower case.

Enough of that lol back to encrypting...

Now we need to open our encrypted file system...

```
sudo cryptsetup luksOpen /dev/loop3 CD
```

Enter in the password you created it with.

Once it tells you that the slot has been unlocked or what ever we need to fill the filesystem up with random bytes to help keep cryptanalyst from guessing what is inside of the cd.

To do that we have a few options in order of most secure to less secure but still works lol...

```
sudo dd if=/dev/random of=/dev/mapper/CD
sudo dd if=/dev/urandom of=/dev/mapper/CD
sudo badblocks -swt random /dev/mapper/CD
```

Pick which ever one you want and use it to fill your filesystem.

Once it is done we need to give our encrypted file system a file system so we can add files...

I like to use ext3...

```
sudo mkfs.ext3 /dev/mapper/CD
```

Now we need to mount our filesystem...

```
mkdir tmp
sudo mount /dev/mapper/CD tmp
```

And change its ownership over to us...

```
sudo chown kenthefurry: tmp -R
chmod 700 tmp -R
```

And now lets get rid of the lost+found directory we don't need it...

```
rm tmp/* -R
```

Woot now we can add files to our filesystem...

So add your super secretive files into it.

Once you have all the files you want to add to that you will have to change a few of the permissions... Not that hard.

```
chmod 444 tmp/* -R
```

```
chmod 555 tmp
```

Now your all set!

So lets unmount the tmp folder we made...

```
sudo umount tmp
```

```
rmdir tmp
```

Lets remove the crypt device mapping...

```
sudo cryptsetup remove CD
```

Now lets clear out loop device...

```
sudo losetup /dev/loop3 -d
```

```
sudo losetup /dev/loop3 /dev/null
```

Now the only thing left to do is to burn it to a disk.

If you are using Ubuntu you will more than likely have a built in ISO burner so go into your work folder and right click on the CD.iso...

Then click Write to CD or what ever it may be.

And your done.

Once it is wrote to the CD eject the CD then put it back In and see if it works, it should on insertion ask you for your password.

If everything works out go ahead and delete your work folder.

I hope this works out for you, if not feel free to email me or pm me on the forums of either UnderGround.mn or anti-forensics.com.

Good Luck.

Shout Outs

- <http://www.underground.mn>

Underground is one of my favorite sites out there. You can find links to any movie, music, or program you want; while being able to chat and have fun; also there is a great support area for any problems a user may face.

- <http://www.anti-forensics.com/>

This is the site that I am making this tutorial for. If you want to try to keep up to date on ways to help keep people out of your computer, this is one of the places to go.

Ubuntu CD/DVD Encryption

The End

Thanks for taking the time to read through this.